

SECURE DIGITAL CONTENT DISTRIBUTION SYSTEM AND SECURE HARD DRIVE

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Application No. 60/485,578, filed on July 8, 2003 and U.S. Provisional Application No. 60/489,361, filed on July 23, 2003, both of which are incorporated herein by reference in their entirety.

FIELD OF THE INVENTION

[0002] The present invention relates to the distribution of digital content such as audio, video, music, still pictures and the like, and more particularly to secure content distribution systems and secure hard drives.

BACKGROUND OF THE INVENTION

[0003] Digital content such as but not limited to computer software, still pictures, audio, music, and video is typically distributed using digital video (or versatile) discs (DVDs), compact discs (CDs), floppy disks, and/or via the Internet. Content providers have had a difficult time preventing piracy of their content. Typically, users store the digital content using hard drives, CDs, DVDs, floppy disks or other electronic storage media. The losses that can be attributed to piracy are well in excess of billions of dollars annually and growing at an alarming pace. Because the medium and the drive are separable, it is very

difficult to defeat bit-by-bit copies of the digital content. For example, pirates of DVDs used bit-by-bit copying before the DVD encryption scheme was cracked.

SUMMARY OF THE INVENTION

[0004] A secure hard drive according to the present invention comprises a storage medium that stores encrypted digital content and corresponding encrypted content keys. A public key decryption module receives one of the encrypted content keys from the storage medium and decrypts the encrypted content key using a private key to generate a content key. A block decryption module receives the encrypted digital content corresponding to the one of the encrypted content keys from the storage medium and the content key from the public key decryption module and decrypts the encrypted content using the content key.

[0005] In other features, the storage medium is a magnetic storage medium. The public key decryption module and the block decryption module are implemented by a system on chip (SOC). A content player receives the decrypted digital content from the block decryption module and generates at least one of an analog output signal and a digital output signal. An identification (ID) module provides an ID. The private key and a public key are based on the ID. A controller performs buffer management and timing of read/write operations.

[0006] A system comprises the secure hard drive and further comprises an external host and a control interface that provides an interface

between the controller and the external host. The external host is one of a computer and a portable media player.

[0007] In yet other features, a watermark detector communicates with an output of the content player and determines whether the analog signal that is output by the content player contains a watermark. The storage medium stores a content directory having content directory entries for the content. The public key decryption module performs digital signature verification of the content directory entry corresponding to the content that is selected for play.

[0008] In other features, at least one of the content directory entries contains a clear content counter that specifies a portion of the corresponding content that is not encrypted. A content distributor identification (ID) field that identifies a content distributor supplying the corresponding content. A content status field that has one of an active status and a passive status. The active status enables playback and the inactive status disables playback. A signature field for the content distributor supplying the corresponding content. A content key location field that contains a first offset value points to a content key for the selected content in a content key block stored on the storage medium. A content location field that contains a second offset value that points to the selected content in an encrypted content block stored on the storage medium.

[0009] In still other features, the content includes at least one of audio, video, and still pictures. The system comprises a distributed communications network and at least one content distributor that transmits encrypted content, an encrypted content key, and a content directory entry for a content selection to the

secure hard drive via the external host and the distributed communications network. The storage medium contains encrypted content that is pre-stored thereon.

[0010] Further areas of applicability of the present invention will become apparent from the detailed description provided hereinafter. It should be understood that the detailed description and specific examples, while indicating the preferred embodiment of the invention, are intended for purposes of illustration only and are not intended to limit the scope of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] The present invention will become more fully understood from the detailed description and the accompanying drawings, wherein:

[0012] FIG. 1 is a functional block diagram of a secure distribution system for digital content according to the present invention;

[0013] FIG. 2 is a functional block diagram illustrating encryption of the digital content and the content key by the content distributor;

[0014] FIG. 3A is a functional block diagram of a secure hard drive that includes a system on chip (SOC) according to the present invention;

[0015] FIG. 3B is a functional block diagram that illustrates one implementation of a controller of FIG. 3A;

[0016] FIG. 4 is a functional block diagram of an exemplary implementation for signing a content directory and/or content directory entry;

[0017] FIG. 5 is a functional block diagram of an alternate implementation for signing a content directory and/or content directory entry;

[0018] FIG. 6 illustrates exemplary fields of a content directory entry;

[0019] FIG. 7 is a flowchart illustrating steps for downloading encrypted digital content from a content distributor;

[0020] FIG. 8 is a flowchart illustrating steps for allowing users to sample portions of inactive content; and

[0021] FIG. 9 is a flowchart illustrating steps for playing back digital content stored on the secure hard drive.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0022] The following description of the preferred embodiment(s) is merely exemplary in nature and is in no way intended to limit the invention, its application, or uses. For purposes of clarity, the same reference numbers will be used in the drawings to identify the same elements. As used herein, the term module refers to an application specific integrated circuit (ASIC), an electronic circuit, a processor (shared, dedicated, or group) and memory that execute one or more software or firmware programs, a combinational logic circuit, and/or other suitable components that provide the described functionality.

[0023] The secure content distribution system according to the present invention integrates the content storage medium with the drive. Since the manufacture of hard drives is a highly specialized industry, a high level of security is provided through this integration. The present invention allows

distribution of a secure personal content library with a low risk of loss of the digital content to piracy.

[0024] Referring now to FIG. 1, a secure content distribution system 10 according to the present invention is shown. The secure content distribution system 10 includes a distributed communications system 14 such as the Internet, a Bluetooth network, a local area network (LAN), a wide area network (WAN), a cellular network, a satellite network or other suitable network. One or more content distributors 18-1, 18-2, ..., and 18-N (collectively content distributors 18) distribute secure digital content such as a software, video, audio, still pictures, music and the like over the distributed communications system 14.

[0025] A network device 22 such as a personal computer, portable media players such as personal digital assistants (PDA), cellular phones, MP3 players, and/or other any other device communicates either wirelessly and/or directly with the content distributors 18 over the distributed communications system 14. The network device facilitates a connection to the content distributors 18. The network device 22 is removably connected to a portable media player 28 that includes a secure hard drive 32. The network device 22 includes a software agent 26 such as a browser that negotiates a link with the content distributor 18 and manages the transfer of data to the secure hard drive 32. The portable media players can also directly connect to the distributed communications system 14. A trusted third party (TTP) distributes and authenticates public keys for the secure hard drives 32 and the content distributors 18. The content distributor 18-3 may also pre-store digital content on

the secure hard drive 32 with either an active status (can be played) or inactive status (cannot be played), as will be described further below.

[0026] Referring now to FIG. 2, when a consumer visits a web site of the content distributor 18, the consumer may wish to purchase content. The content distributor 18 uses an encryption module 50 that encrypts content 54 using a content key 56. The content key 56 is preferably a randomly selected key, although other methods for determining content keys may be used. The content key 56 is then encrypted using a public key 58 of the secure hard drive 32 that requests the content 54. The consumer downloads encrypted content 60 and an encrypted content key 64 over the distributed communications system 14 onto the secure hard drive 32.

[0027] Referring now to FIG. 3A, the secure hard drive 32 is shown in further detail and includes a SOC 70 and a magnetic medium 72, which stores the encrypted content 60 and the encrypted content keys 64. While the SOC 70 is shown, components of the SOC 70 can be implemented as discrete components. As will be described below, only the SOC on the secure hard drive 32 can recover the content key 56. The SOC 70 includes a control interface 74 that provides an external interface to a host and/or network device. The control interface 74 communicates with a controller 76, which performs buffer management, times read/write events and performs other hard drive operations. The controller 76 may include one or more of the following components: a central processing unit (CPU), memory, a hard drive controller (HDC), a buffer manager, firmware, a universal serial bus (USB), and/or other components.

[0028] The controller 76 communicates with a read channel circuit 80 and a preamplifier 82, which recover the data from the read signal that is generated by the read/write head as it passes over the magnetic medium 72. The read signal is processed by the read channel 80 and the controller 76 to generate digital data signals. Some of the digital data signals include the encrypted content key 64, which is output to a public key decryption module 84. A chip ID module 86 outputs a chip ID to the public key decryption module 84. The SOC 70 has a unique chip ID, which is used to generate a private key for the SOC 70. The private key, in turn, is used to generate a public key for the SOC 70. For example, the public key decryption module 80 may contain a sub-module that converts the Chip-ID to the private key. Various algorithms may be used to generate the private key.

[0029] The public key decryption module 84 uses the private key of the SOC 70 to decrypt the encrypted content key 64 and outputs the content key 56 to a block decryption module 90. The controller 76 outputs the encrypted content 60 to the block decryption module 90, which uses the content key 56 to decrypt the encrypted content 60. The block decryption module 90 outputs the content to a content player 88, which generates an analog and/or digital output signal that includes at least one of audio, video, still pictures, and the like.

[0030] The SOC 70 may optionally include a watermark detector 92 that determines whether the analog signal that is output by the content player 88 includes a watermark. The watermark includes copy control information

embedded in the analog signal. In other words, the watermark detector 92 is used to defeat analog attacks such as capture and re-coding.

[0031] Referring now to FIG. 3B, one implementation of the controller 76 is shown to include a serial and/or parallel interface 94 such as but not limited to serial ATA and/or Integrated Device Electronics (IDE), a hard disk controller (HDC) 96, a buffer 98, a spindle voice coil module (VCM) 100, and a processor 102. The spindle VCM 100, which interfaces with the HDC 96 and a spindle motor 104, controllably rotates the magnetic medium 72. The spindle VCM 100 also interfaces with a read/write arm 106 that is used to position a magneto-resistive (MR) head 108. A resistance of the MR head 108 varies as it passes in proximity to stored positive and negative magnetic fields on the magnetic medium 72, which represent digital ones and zeros. The buffer 98 stores data that is associated with read/write operations and other control functions of the controller 76. The processor 102 performs processing that is associated with the read/write operations and other functions of the controller 76. While a specific implementation is shown for the controller 76, skilled artisans will appreciate that there are other suitable controller configurations that are contemplated.

[0032] Referring now to FIG. 4, processing of the content directory is shown in further detail. The content distributor 18 creates a content directory and/or a content directory entry for the selected content. The content directory entry may include data such as but not limited to the title, artist, and status (active (can be played) and inactive (cannot be played)). The content directory is

preferably protected by a digital signature of the content distributor 18 so that others cannot modify the fields that are stored in the content directory.

[0033] The content distributor 18 may use an encryption module 120 and a private key 122 to sign the content directory and/or the content directory entry. A signed content directory 126 is transmitted over the distributed communications system 14 or otherwise input to the secure hard drive 32. For example, one implementation where the distributed communications system 14 is not used includes a secure hard drive 32 with pre-recorded content. The pre-recorded content may be inactive (cannot be played) or active (can be played).

[0034] The secure hard drive 32 includes a decryption module 130, which uses the public key 132 of the content distributor 18 to generate a verified content directory 134 from the signed content directory 126. While others may view the signed content directory 126, they are unable to modify it. While this is an effective method for securing the content directory 124, the signed content directory 126 is typically at least twice the size of the content directory 124.

[0035] An alternate implementation for signing the content directory 124 is shown in FIG. 5. A one-way hash module 140 uses a hash function to generate a digest 141 from the content directory 124. The digest is then signed with a private key of the content distributor 18 in an encryption module 142. The plaintext content directory 124 is also transmitted or otherwise loaded on the secure hard drive 32. The secure hard drive 32 includes a decryption module 150 that uses the public key of the content distributor 18 to recover the digest 141. The secure hard drive 32 also includes a one-way hash module 140 that

generates a calculated digest. The two digests (the recovered digest and the hash-generated digest) are compared by a comparing module 154, which generates a valid digest signal if they match and an invalid digest signal if they do not. Both the secure hard drive 32 and the content distributor 18 preferably maintain a copy of the content directory. If the secure hard drive 32 fails, all of the digital content that is owned by the consumer can be replaced after proper verification.

[0036] Referring now to FIG. 6, an exemplary content directory entry 160 is shown. Skilled artisans will appreciate that the content directory will contain an entry for each content selection. The content directory entry 160 includes a content distributor identification (ID) field 162 that identifies the content distributor 18. Content title and artist fields 164 and 166 describe the title of the content and name of the artist, respectively. A content status field 168 identifies whether the content is active or inactive. A clear content counter 172 specifies a predetermined portion (bits, bytes, segments and/or any other measure) at the beginning of the digital content that is not encrypted. The clear content counter 172 is specified by the content distributor 18.

[0037] A key hash value field 174 contains a hash value. The encrypted content key can be hashed and the hash value can be protected by the content distributor's signature. The key hash value is used to defeat a possible hacker. For example, without this field, a hacker can purchase one content selection (active) and have other inactive content selections. The hacker could play the inactive content selections by replacing the content location and

the content key location fields in the inactive content directory entries with the content location and content key location of the active content selection. A secure hard drive without the hash field may allow this to occur. If the key hash value field is used, this approach will be prevented.

[0038] A content distributor's signature field 176 contains the signature of the content distributor, which can be verified using the content distributor's public key. The content key location field 178 contains an offset value that points to a selected content key 180 in a content key data block 182. A content location field 184 contains an offset value that points to encrypted content 186 in an encrypted data block 190. The fields 178 and 184 will typically be determined by the secure hard drive 32 rather than the content distributor 18.

[0039] Referring now to FIG. 7, typical steps that are implemented by the content distributor 18 for secure content distribution according to the present invention are shown. A consumer visits a website of the content distributor 18 in step 200. In step 202, the content distributor 18 determines whether the consumer purchases content. If step 202 is true, the content distributor 18 encrypts the selected digital content with the random content key and sends the encrypted content to the secure hard drive 32 in step 204.

[0040] In step 208, the content distributor 18 encrypts the content key with the public key of the secure hard drive 32 and sends the encrypted content key to the secure hard drive 32. As can be appreciated, the encrypted content and the encrypted content key can be sent to the purchasing consumer at the same time. The content directory may be signed and sent at this time using the

methods described above. In step 210, the content distributor 18 determines whether the consumer exits the website of the content distributor. If yes, control ends. Otherwise, control returns to step 202.

[0041] Referring now to FIG. 8, operation of the clear content counter in the secure hard drive 32 is illustrated. In step 220, the secure hard drive 32 determines whether the user selects content for play. If not, control loops back to step 220. Otherwise when the user selects content to be played, the secure hard drive 32 determines whether the content has a content status that is equal to active in step 222. If true, the secure hard drive 32 plays the content in step 223. Otherwise, control determines whether the clear content counter is greater than zero in step 224. If not, control sends a message to the user that the content is not active and that a sample is not available in step 225. If step 224 is true, a counter is set to zero in step 226. In step 228, the content is played and the counter is incremented. In step 230, the secure hard drive 32 determines whether the counter is greater than the clear content counter. If false, control continues with step 228. Otherwise the sample time is over when the counter exceeds the clear content counter. A message is sent to the user that the sample is over in step 234. Additional steps and/or dialogue may be initiated with the user to solicit purchase of the sampled digital content. Steps 225 and 234 may be omitted if desired.

[0042] Referring now to FIG. 9, steps for playing back content are shown. In step 250, control determines whether the consumer selects content for playback. If not, control loops back to step 250. In step 252, control retrieves

the encrypted content key, the content directory entry and the encrypted content that are associated with the selected content. In step 254, the digital signature is verified. In step 256, control determines whether the digital signal is valid. If not, control ends in step 257. Otherwise control continues with step 258 and the content key is decrypted with the private key of the secure hard drive 32. In step 260, the content is decrypted using the decrypted content key. In step 264, an analog signal is generated from the decrypted content and is output to an audio and/ video playback device. In step 266, control determines whether a watermark is detected (when the optional watermark detector is used). If not, control ends in step 257. Otherwise, control determines whether the selected content is over. If not, control ends in step 257. Otherwise control loops back to step 260.

[0043] There are many advantages when content is distributed using the secure hard drive 32 and the secure content distribution system 10 according to the present invention. The content distributors 18 have end-to-end control of the encryption of their digital content. The content key is not revealed to anyone else on the network other than the content distributor 18. On the consumer side, the content key is never revealed outside of the SOC 70. Security is not compromised even if a hacker hacks into the firmware of the secure hard drive 32. The chip-ID is part of a very complicated chip (the SoC). Therefore, it would take a significant amount of effort to determine the chip-ID. Even if the hacker can determine the chip-ID, it is still very difficult to determine the private key from the chip-ID. For example, a keyed-hash function and/or other coding techniques

can be used to generate the private key from the chip-ID. Therefore, the system cannot be compromised without breaking the encryption/decryption scheme, which is unlikely.

[0044] Those skilled in the art can now appreciate from the foregoing description that the broad teachings of the present invention can be implemented in a variety of forms. For example, while the present invention is described in conjunction with magnetic storage systems, other electronic storage may be used such as memory and/or optical storage. Therefore, while this invention has been described in connection with particular examples thereof, the true scope of the invention should not be so limited since other modifications will become apparent to the skilled practitioner upon a study of the drawings, the specification and the following claims.